Romain Jacquet **BTS SIO 1**

13/01/2026

Compte rendu TP Message secret sous ubuntu...

Sommaire

Introduction

Pour ce TP sous Ubuntu, le but était d'apprendre à sécuriser un système de manière ludique en défiant un binôme. J'ai dû imaginer et mettre en place une stratégie complète pour dissimuler un "message secret" (création d'utilisateur, gestion des permissions, suppression de traces), le défi étant de rendre ce fichier impossible à trouver ou à lire pour mon camarade.

Mission 1 Cacher le mot secret

1. J'ai créé le "Gardien" et son dossier caché

J'ai commencé par créer un utilisateur dédié nommé "gardien" et une arborescence contenant un dossier caché.

```
# J'ai créé le nouvel utilisateur 'gardien'
sudo adduser gardien

# Je me suis connecté en tant que ce nouvel utilisateur
su - gardien

# J'ai créé un dossier caché (le point devant le nom le rend invisible)
mkdir .base_secrete
```

2. J'ai créé et archivé le secret

J'ai rédigé mon message, puis je l'ai compressé au format `tar.gz` pour l'isoler.

```
# J'ai créé le fichier contenant le message secret
echo "Le code secret est 1234" > .base_secrete/message.txt

# J'ai compressé le fichier (c=create, z=gzip, v=verbose, f=file)
tar -czvf .base_secrete/archive_secrete.tar.gz .base_secrete/message.txt
```

3. J'ai protégé le fichier avec des permissions strictes

J'ai appliqué des droits d'accès restreints (`chmod 600` ou `700`) pour m'assurer que personne d'autre ne puisse lire l'archive.

```
# J'ai limité l'accès au fichier (lecture/écriture pour moi uniquement)
chmod 600 .base_secrete/archive_secrete.tar.gz

# J'ai sécurisé l'accès au dossier lui-même
chmod 700 .base_secrete
```

4. J'ai brouillé les pistes

Pour terminer, j'ai supprimé le fichier texte original (fichier temporaire) et je n'ai laissé qu'un seul indice pour orienter la recherche.

```
# J'ai supprimé le fichier message original non compressé
rm .base_secrete/message.txt

# J'ai laissé un indice pour mon binôme
echo "Cherche l'archive cachée du gardien..." > indice.txt
```

5. J'ai supprimé les traces (l'historique des commandes)

Pour finir, j'ai effacé la liste des commandes que je venais de taper. Cela empêche mon binôme de retrouver le fichier secret simplement en regardant l'historique ou en appuyant sur la "flèche du haut". C'est l'étape ultime pour "brouiller les pistes".

```
# J'ai effacé l'historique de la session en cours
history -c

# J'ai vidé le fichier qui enregistre toutes les commandes
cat /dev/null > ~/.bash_history

# Je me suis déconnecté pour valider le nettoyage
exit
```

Mission 2 Trouver le mot secret

La mission 2 a été réalisé par mon binôme (il n’a pas réussi à trouver le mot secret car il lui as manqué du temps)

Conclusion

En conclusion, cet exercice m'a fait réaliser qu'il ne suffit pas de cacher un fichier pour le protéger, mais qu'il faut surtout bien verrouiller les droits d'accès. J'ai réussi ma mission de défense puisque mon binôme n'a pas trouvé mon fichier, ce qui m'a prouvé l'efficacité concrète des commandes de sécurité et du nettoyage d'historique que j'ai utilisées.